

By Donald A. Glazier and Jim Dunn

## Predicting the Unpredictable

Viruses, malware and spyware of all types—Trojan Horses, worms, resident, direct action, overwrite, boot, macro, directory, polymorphic, system attacks, spam and e-mail overload, denial of service—reside in the quiver of the typical computer hacker. And now hackers have added a new selection to their repertoire—instead of destroying entire systems, they are uploading inappropriate, illegal images to unsuspecting parties' computers<sup>1</sup>. Victims of this latest scheme are unwittingly associated with problematic content. If this happens in the workplace, an employer may need to expend considerable time, energy and dollars to determine the innocence or guilt of an affected party.

This latest hazard illustrates why cyber-risks represent a "moving target." On an almost daily basis, the subject matter, design and delivery of cyber perils may change. While the probability, if not certainty, of cyber liability is axiomatic, the type of incident and associated impact are far less predictable. It is therefore prudent to be familiar with frequent and fundamental cyber perils and the insurance products that have been designed to address them.

## The Painful Financial Price of Cyber Perils

### Denial of service or cyber-vandalism attacks

Whether your company is victimized by an outside hacker or by an internal employee, the financial consequences of a system failure can be severe. For example, the cost of lost business associated with the recent PayPal outage is estimated to be between \$7 million to \$32 million in lost revenue. In addition to lost productivity and sales, the price of system changes or additional preventative software is also high. A large grocer recently spent "millions" to upgrade security after four million credit cards were stolen.<sup>2</sup>

### Data breach / information theft

Failing to safeguard data is expensive. Regardless of whether an employee throws personal data records into a dumpster, or a thief steals a laptop and then destroys or discloses similar data, almost every state in the United States requires notification for such breach events.<sup>3</sup>

The Ponemon Institute estimates the cost of a data breach at \$202 per victim<sup>4</sup>. This number includes elements of detection and escalation (\$8), notification (\$15), ex-post response, such as credit-monitoring services (\$39), and lost business (\$139).

---

<sup>1</sup> Associated Press, "[Framed for child porn by a PC virus](#)," Jordan Robertson, Nov 8, 2009.

<sup>2</sup> The Washington Post, "Hannaford's Breach Tests Limits of Security Controls," Brian Krebs, April 23, 2008.

<sup>3</sup> By the third quarter of 2009, 45 states require notification of security breaches involving personal information. [National Conference of State Legislatures, July 2009](#).

<sup>4</sup> Ponemon Institute, "[Fourth Annual US Cost of Data Breach Study](#)," January 2009.

With an estimated 35 million records exposed in 2008<sup>5</sup>, that is more than \$7 billion of potential costs for reported incidents alone.

Another factor to consider is any associated regulatory redress ensuing from the breach. Under the Fair Credit Reporting Act, companies who recklessly store data could be liable for up to \$1,000 per victim.<sup>6</sup> Additionally, litigation arising from a breach incident may be costly to defend or settle. For example, a large retailer recently agreed to pay over \$40 million to banks and credit unions following a breach incident.<sup>7</sup>

### **Spreading Malware to Customers or Vendors**

Connectivity is a blessing and a curse. While online connections make it easier to transact business with customers and vendors, it unfortunately also makes it easier to unwittingly transfer cyber-bugs as well.

### **Cyber Extortion**

Some hackers are motivated by malice, revenge, or even potential fame. Others are motivated by money. These cyber-extortionists may threaten to destroy an entire system unless payments are made. In a recent example, a prescription processing firm offered a \$1 million bounty for information leading to the arrest and conviction of a group that threatened to release millions of personal records unless ransom monies were received.

## **A Maturing Insurance Marketplace with Affordable Solutions**

As cyber exposure evolves, so too do insurance products designed to address the risk. Coverage offerings and the cost of cyber and privacy insurance policies continue to change rapidly. Given the moving target nature of the risk, insurers' policy offerings approach coverage from varying perspectives, crafting significantly unique policy structures and wordings. These different approaches underscore the need to engage the assistance of an experienced broker well versed in this specialty area, who can help select the most appropriate insurance protection to meet your needs and expectations.

Despite the different approaches to coverage, certain core elements are offered by almost all insurers in this area and should be considered to appropriately address universal cyber and privacy risks. Some of these basic coverages include the following:

### **Physical Damage and Business Interruption Cost Coverage**

- First party coverage that pays for the costs and losses caused by certain attacks on computer networks. Commonly covered losses include loss of business income, data restoration cost, extortion payments, computer forensic and crisis management expenses. Only a select number of carriers

---

<sup>5</sup> According to [The Identity Theft Resource Center](#), "the number of records reported exposed in 2008 was over 35 million records."

<sup>6</sup> 15 U.S.C. §1681(a)(1)(A).

<sup>7</sup> SC Magazine, "TJX agrees to \$41 million settlement with Visa," Frank Washkuch Jr., November 3, 2007.

include this coverage in their property forms. It is typically offered as an “add on” with limits from \$250,000 to \$5 million for an additional premium. Extortion payments and crisis management expenses generally are not recoverable under the property form, but may be available through third party cyber insurance products.

#### **Privacy Breach Notice Cost Coverage**

- Pays the costs associated with complying with the privacy breach notice laws present in the vast majority of states. Insurers also offer coverage for credit monitoring costs and security breach experts who can assist in locating and preventing the problem.

#### **Electronic Media Liability**

- Protects against claims for website related exposures such as trademark or copyright infringement as well as libel and slander, invasion of privacy, and plagiarism. Also addresses negligence.

#### **Computer Information Security**

- Provides coverage for third party claims alleging theft, loss or improper disclosure of personally identifiable information.
- Insures against claims arising from unauthorized access, theft or destruction of data, i.e., hacker protection.

#### **Cyber Extortion Coverage**

- Covers the costs of payments associated with threats to destroy a network or release private information.

A purchaser of a cyber-privacy policy can pick and choose from these core coverages as well as additional coverage offerings that are appropriate for its business, customizing a policy that combines elements of both liability and property policies.

### **The Time is Right**

As the cyber coverage marketplace matures, pricing has become more favorable for insureds. This, in turn, has increased demand among companies who at first eschewed the coverage due to pricing concerns. As the number of participants underwriting the coverage has grown, competition has expanded coverage and driven down pricing for attractive risks.

Even in a softening marketplace, making a purchasing decision about cyber-privacy coverage requires the services of a knowledgeable broker. At Integro, we can provide guidance through the complicated thicket of policy offerings. Our brokers are well experienced in helping clients obtain the most appropriate policy and avoid — avoiding any gaps in coverage. Integro offers our clients keen broker knowledge plus coverage support from counsel experienced in this area.

---

**Jim Dunn** is a Principal in Integro's New York office with over 28 years' experience in property program design, pre-loss and post loss claim management. He is a skilled negotiator who is highly respected in the marketplace. Jim's clients represent various industries, including financial institutions, real estate, hospitality and entertainment, heavy manufacturing, retail, chemical, petrochemical risks and telecommunications.

**Donald A. Glazier** is a Principal with the Management Risk Practice operating from Integro's Chicago office. An attorney by background, he specializes in professional liability issues.

**Tara L. Cummins** assisted Jim and Don in the preparation of this article. Tara is a Senior Associate in the Management Risk Practice in the New York office. Also an attorney by background, she specializes in knowledge management.

**About Integro**

Integro is an insurance brokerage and risk management firm dedicated to serving the insurance and risk management needs of complex institutional risks. Integro has offices across North America, as well as in Bermuda and London. Its headquarter office is located at 1 State Street, 9th Floor, New York NY 10004. 1-877-688-8701. [www.integrogroup.com](http://www.integrogroup.com).

Copyright 2010, Integro USA Inc.